

# REAL ALGEBRAIC GEOMETRY FOR GEOMETRIC CONSTRAINTS

FRANK SOTTILE

ABSTRACT. Real algebraic geometry adapts the methods and ideas from (complex) algebraic geometry to study the real solutions to systems of polynomial equations and polynomial inequalities. As it is the real solutions to such systems modeling geometric constraints that are physically meaningful, real algebraic geometry is a core mathematical input for geometric constraint systems.

## 1. INTRODUCTION

Algebraic geometry is fundamentally the study of sets, called *varieties*, which arise as the common zeroes of a collection of polynomials. These include familiar objects in analytic geometry, such as conics, plane curves, and quadratic surfaces. Combining

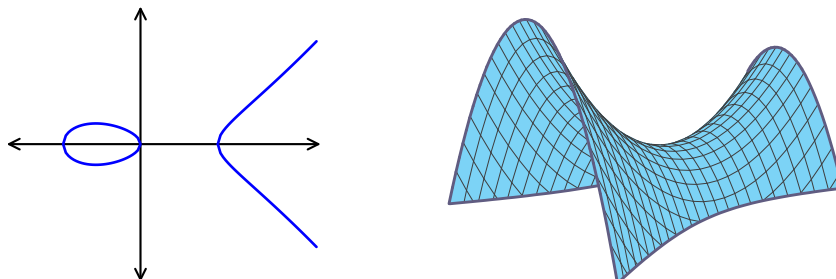


FIGURE 1. A cubic plane curve and a quadratic surface (a hyperbolic paraboloid)

intuitive geometric ideas with precise algebraic methods, algebraic geometry is equipped with many powerful tools and ideas. These may be brought to bear on problems from geometric constraint systems because many natural constraints, particularly prescribed incidences, may be formulated in terms of polynomial equations.

Consider a four-bar mechanism; a quadrilateral in the plane with prescribed side lengths  $a$ ,  $b$ ,  $c$ , and  $d$ , which may rotate freely at its vertices and where one edge is fixed as in Figure 2. The points  $x$  and  $y$  are fixed at a distance  $a$  apart, the point  $p$  is constrained to lie on the circle centered at  $x$  with radius  $b$ , the point  $q$  lies on the circle centered at  $y$  with radius  $c$ , and we additionally require that  $p$  and  $q$  are a distance  $d$  apart. Squaring the distance constraints gives a system of three quadratic equations whose solutions are all positions of this four-bar mechanism.

Algebraic geometry works best over the complex numbers, because the geometry of a complex variety is controlled by its defining equations. (For instance, the Fundamental

---

2010 *Mathematics Subject Classification*. 14P99, 14Q20.

Research of Sottile supported in part by NSF grant DMS-1501370.

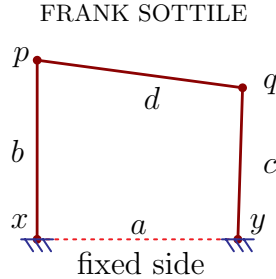


FIGURE 2. A four-bar mechanism

Theorem of Algebra states that a univariate polynomial of degree  $n$  always has  $n$  complex roots, counted with multiplicity.) Geometric constraint systems are manifestly real (as in real-number) objects. For this reason, the subfield of *real algebraic geometry*, which is concerned with the real solutions to systems of equations, is most relevant for geometric constraint systems. Working over the real numbers may give quite different answers than working over the complex numbers.

This chapter will develop some parts of real algebraic geometry that are useful for geometric constraint systems. Its main point of view is that one should first understand the geometry of corresponding complex variety, which we call the *algebraic relaxation* of the original problem. Once this is understood, we then ask the harder question about the subset of real solutions.

For example,  $x^2 + y^2 = 1$  and  $x^2 + y^2 = -1$  define isomorphic curves in the complex plane—send  $(x, y) \mapsto (\sqrt{-1}x, \sqrt{-1}y)$ —which are quite different in the real plane. Indeed,  $x^2 + y^2 = 1$  is the unit circle in  $\mathbb{R}^2$  and  $x^2 + y^2 = -1$  is the empty set. Replacing  $\pm 1$  by 0 gives the pair of complex conjugate lines

$$x^2 + y^2 = (x + \sqrt{-1}y)(x - \sqrt{-1}y) = 0,$$

whose only real point is the origin  $(0, 0)$ . The reason for this radically different behavior amongst these three quadratic plane curves is that only the circle has a smooth real point—by Theorem 5.1, when a real algebraic variety has a smooth real point, the salient features of the underlying complex variety are captured by its real points.

## 2. IDEALS AND VARIETIES

The best accessible introduction to algebraic geometry is the classic book of Cox, Little, and O’Shea [7]. Many thousands find this an indispensable reference. We assume a passing knowledge of some aspects of the algebra of polynomials, or at least an open mind. We work over the complex numbers,  $\mathbb{C}$ , for now. A collection  $S \subset \mathbb{C}[x_1, \dots, x_d]$  of polynomials in  $d$  variables defines a *variety*,

$$\mathcal{V}(S) := \{x \in \mathbb{C}^d \mid f(x) = 0 \text{ for all } f \in S\}.$$

We may add to  $S$  any of its polynomial consequences,  $g_1 f_1 + \dots + g_s f_s$  where  $g_i \in \mathbb{C}[x_1, \dots, x_d]$  and  $f_i \in S$ , without changing  $\mathcal{V}(S)$ . This set of polynomial consequences is the *ideal generated by  $S$* , and so it is no loss to assume that  $S$  is an ideal. Hilbert’s Basis Theorem states that any ideal in  $\mathbb{C}[x_1, \dots, x_d]$  is finitely generated, so it is also no loss to assume that  $S$  is finite. We pass between these extremes when necessary.

Dually, given a variety  $X \subset \mathbb{C}^d$  (or any subset), let  $\mathcal{I}(X)$  be the set of polynomials which vanish on  $X$ . Any polynomial consequence of polynomials that vanish on  $X$  also vanishes on  $X$ . Thus  $\mathcal{I}(X)$  is an ideal in the polynomial ring  $\mathbb{C}[x_1, \dots, x_d]$ . Let  $\mathbb{C}[X]$  be the set of functions on  $X$  that are restrictions of polynomials in  $\mathbb{C}[x_1, \dots, x_d]$ . Restriction is a surjective ring homomorphism  $\mathbb{C}[x_1, \dots, x_d] \twoheadrightarrow \mathbb{C}[X]$  whose kernel is the ideal  $\mathcal{I}(X)$  of  $X$ , so that  $\mathbb{C}[X] = \mathbb{C}[x_1, \dots, x_d]/\mathcal{I}(X)$ . Call  $\mathbb{C}[X]$  the coordinate ring of  $X$ .

To see this connection between algebra and geometry, consider the two plane curves  $\mathcal{V}(y - x^2)$  and  $\mathcal{V}(y^2 - x^3)$  of Figure 3. One is the familiar parabola, which is smooth, and

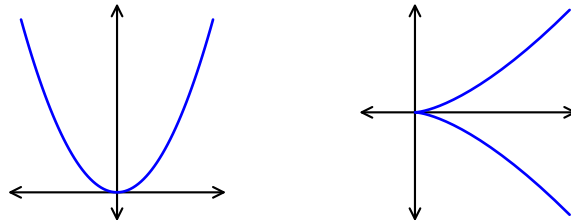


FIGURE 3. Plane curves  $\mathcal{V}(y - x^2)$  and  $\mathcal{V}(y^2 - x^3)$

the other the semicubical parabola or cuspidal cubic, which is singular (see § 4.2) at the origin. Their coordinate rings are  $\mathbb{C}[x, y]/\langle y - x^2 \rangle$  and  $\mathbb{C}[x, y]/\langle y^2 - x^3 \rangle$ , respectively. The first is isomorphic to  $\mathbb{C}[t]$ , which is the coordinate ring of the line  $\mathbb{C}$ , while the second is not—it is isomorphic to  $\mathbb{C}[t^2, t^3]$ . The isomorphisms come from the parameterizations  $t \mapsto (t, t^2)$  and  $t \mapsto (t^2, t^3)$ . This illustrates another way to obtain a variety—as the image of a polynomial map.

Thus begins the connection between geometric objects (varieties) and algebraic objects (ideals). Although they are different objects, varieties and ideals carry the same information. This is expressed succinctly and abstractly by stating that there is an equivalence of categories, which is a consequence of Hilbert’s Nullstellensatz, whose finer points we sidestep. For the user, this equivalence means that we may apply ideas and tools either from algebra or from geometry to better understand the sets of solutions to polynomial equations.

### 3. ... AND ALGORITHMS

Because the objects of algebraic geometry have finiteness properties (finite-dimensional, finitely generated), they may be faithfully represented and manipulated on a computer. There are two main paradigms: symbolic methods based on Gröbner bases and numerical methods based on homotopy continuation. The first operates on the algebraic side of the subject and the second on its geometric side.

A consequence of the Nullstellensatz is that we may recover any information about a variety  $X$  from its ideal  $\mathcal{I}(X)$ . By Hilbert’s Basis Theorem,  $\mathcal{I}(X)$  is finitely generated, so we may represent it on a computer by a list of polynomials. We emphasize computer because expressions for multivariate polynomials may be too large for direct human manipulation or comprehension. Many algorithms to study a variety  $X$  through its ideal begin with a preprocessing: a given list of generators  $(f_1, \dots, f_m)$  for  $\mathcal{I}(X)$  is replaced by another

list  $(g_1, \dots, g_s)$  of generators, called a *Gröbner basis* for  $\mathcal{I}(X)$ , with optimal algorithmic properties. Buchberger’s Algorithm is a common method to compute a Gröbner basis.

Many algorithms to extract information from a Gröbner basis have reasonably low complexity. These include algorithms that use a Gröbner basis to decide if a given polynomial vanishes on a variety  $X$  or to determine the dimension or degree (see § 4.1 and § 4.2) of  $X$ . Consequently, a Gröbner basis for  $\mathcal{I}(X)$  transparently encodes much information about  $X$ . We expect, and it is true, that computing a Gröbner basis may have high complexity (double exponential in  $d$  in the worst case), and some computations do not terminate in a reasonable amount of time. Nevertheless, symbolic methods based on Gröbner bases easily compute examples of moderate size, as the worst cases appear to be rare.

Several well-maintained computer algebra packages have optimized algorithms to compute Gröbner bases, extensive libraries of implemented algorithms using Gröbner bases, and excellent documentation. Two in particular—Macaulay2 [11, 12] and Singular [8, 9]—are freely available with dedicated communities of users and developers. Commercial software, such as Magma, Maple, and Mathematica, also compute Gröbner bases and implement some algorithms based on Gröbner bases. Many find SageMath [10], an open-source software connecting different software systems together, also to be useful.

The other computational paradigm—numerical algebraic geometry—uses methods from numerical analysis to manipulate varieties on a computer [18]. Numerical homotopy continuation is used to solve systems of polynomial equations, and Newton’s method may be used to refine the solutions. These methods were originally developed as a tool for mechanism design in kinematics [15], which is closely related to geometric constraint systems.

In numerical algebraic geometry, a variety  $X$  of dimension  $n$  (see § 4.2) in  $\mathbb{C}^d$  is represented on a computer by a *witness set*, which is a triple  $(W, S, L)$ , where  $L$  is a general affine plane in  $\mathbb{C}^d$  of dimension  $d-n$ ,  $S$  is a list of polynomials defining  $X$ , and  $W$  consists of numerical approximations to the points of  $X \cap L$  (the number of which is the degree of  $X$ , see § 4.2). Following the points of  $W$  as  $L$  varies using homotopy continuation samples points of  $X$ , and may be used to test for membership in  $X$ . Other algorithms, including computing intersections and the image of a variety under a polynomial map, are based on witness sets.

Two stand-alone packages—PHCPack [22] and Bertini [3, 2]—implement the core algorithms of numerical algebraic geometry, as does the Macaulay2 package NAG4M2 [14]. Both PHCPack and Bertini may be accessed from Macaulay2, Singular, or SageMath.

Each computational paradigm, symbolic and numerical, has its advantages. Symbolic computations are exact and there are many implemented algorithms. The inexact numerical computations give refinable approximations, yielding a family of well-behaved relaxations to exact computation. Also, numerical algorithms are easily parallelized and in some cases the results may be certified to be correct [13, 17].

#### 4. STRUCTURE OF ALGEBRAIC VARIETIES

Varieties and their images under polynomial maps have well-understood properties that may be exploited to understand objects modeled by varieties. We discuss some of these fundamental and structural properties.

4.1. **Zariski Topology.** Algebraic varieties in  $\mathbb{C}^d$  are closed subsets in the usual (classical) topology because polynomial functions are continuous. Varieties possess a second, much coarser topology—the Zariski topology—whose value is that it provides the most natural language for expressing many properties of varieties. The Zariski topology is determined by its closed sets, which are simply the algebraic varieties, and therefore its open sets are complements of varieties.

Closure in the Zariski topology is easily expressed: The Zariski closure  $\overline{U}$  of a set  $U \subset \mathbb{C}^d$  is  $\mathcal{V}(\mathcal{I}(U))$ , the set of points in  $\mathbb{C}^d$  where every polynomial that vanishes identically on  $U$  also vanishes. A non-empty Zariski open subset  $U$  of  $\mathbb{C}^d$  is dense in  $\mathbb{C}^d$  in the classical topology, and a classical open subset of  $\mathbb{C}^d$  (e.g. a ball) is dense in the Zariski topology. The Zariski topology of a variety  $X$  in  $\mathbb{C}^d$  is induced from that of  $\mathbb{C}^d$ .

We use the Zariski topology to express the analog of unique factorization of integers for varieties. A variety  $X$  is *irreducible* if cannot be written as a union of proper subvarieties. That is, if  $X = Y \cup Z$  with  $Y, Z$  subvarieties of  $X$ , then either  $X = Y$  or  $X = Z$ . A variety  $X$  has an irredundant decomposition into irreducible subvarieties,  $X = X_1 \cup \dots \cup X_m$ , which is unique in that each  $X_i$  is an irreducible subvariety of  $X$  and if  $i \neq j$ , then  $X_i \not\subset X_j$ . We call the subvarieties  $X_1, \dots, X_m$  the (*irreducible*) *components* of  $X$ .

This decomposition for a hypersurface is equivalent to the factorization of its defining polynomial into irreducible polynomials. For the curve on the left in Figure 4 we have,

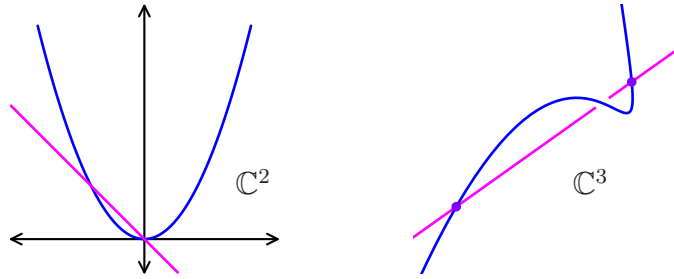


FIGURE 4.  $\mathcal{V}(x^3+x^2y-xy-y^2)$  and  $\mathcal{V}(z-xy, xz-y^2-x^2+y)$

$$x^3 + x^2y - xy - y^2 = (x^2 - y)(x + y),$$

showing that its components are the parabola  $y = x^2$  and the line  $y = -x$ . Both  $\mathcal{V}(x^3+x^2y-xy-y^2)$  and  $\mathcal{V}(z-xy, xz-y^2-x^2+y)$  are curves with two components, as we see in Figure 4.

Zariski open sets are quite large. Any nonempty Zariski open subset  $U$  of an irreducible variety  $X$  is Zariski dense in  $X$ . Indeed,  $X = \overline{U} \cup (X \setminus U)$ , the union of two closed subsets. Since  $X \neq X \setminus U$ , we have  $\overline{U} = X$ . In fact,  $U$  is dense in the classical topology, and any subset of  $X$  that is dense in the classical topology is Zariski dense in  $X$ .

A property of an irreducible variety  $X$  is *generic* if the set of points where that property holds contains a Zariski open subset of  $X$ . Generic properties of  $X$  hold almost everywhere on  $X$  in a very strong sense, as the points of  $X$  where they do not hold lie in a proper subvariety of  $X$ . A point of a variety where a generic property holds is *general* (with respect to that property).

**4.2. Smooth and Singular Points.** Algebraic varieties are not necessarily manifolds, as may be seen in Figures 3 and 4. However, the set of points where a variety fails to be a manifold is a proper subvariety. To see this, suppose that  $X \subset \mathbb{C}^d$  is a variety whose ideal  $\mathcal{I}(X)$  has generators  $f_1, \dots, f_s$ . At each point  $x$  of  $X$ , the Jacobian matrix  $J = (\partial f_i / \partial x_j)_{\substack{j=1, \dots, d \\ i=1, \dots, s}}$  has rank between 0 and  $d$ . The set  $X_i$  of points of  $X$  where the rank of  $J$  is at most  $i$  is a subvariety which is defined by the vanishing of all  $(i+1) \times (i+1)$  minors of  $J$ . If  $i$  is the smallest index such that  $X_i = X$ , so that  $X_{i-1} \subsetneq X$ , then at every point of  $X_{\text{sm}} := X \setminus X_{i-1}$  the Jacobian has rank  $i$ . Differential geometry informs us that  $X_{\text{sm}}$  is a complex manifold of dimension  $d-i$ .

When  $X$  is irreducible,  $X_{\text{sm}}$  is the set of smooth points of  $X$  and  $X_{\text{sing}} := X \setminus X_{\text{sm}}$  is the *singular locus* of  $X$ . A point being smooth is a generic property of  $X$ . The *dimension*  $\dim X$  of an irreducible variety  $X$  is the dimension of  $X_{\text{sm}}$ . When  $X$  is reducible, its dimension is the maximum dimension of an irreducible component. The singular locus of a variety  $X$  always has smaller dimension than  $X$ .

For algebraic varieties, dimension has the following properties. If  $X$  and  $Y$  are subvarieties of  $\mathbb{C}^d$  of dimensions  $m$  and  $n$ , respectively, then either  $X \cap Y$  is empty or every irreducible component of  $X \cap Y$  has at least the expected dimension  $m+n-d$ . For a general translate  $Y'$  of  $Y$ ,  $\dim(X \cap Y') = m+n-d$ . More precisely, there is a Zariski open subset  $U$  of the group  $\mathbb{C}^d \rtimes GL(d, \mathbb{C})$  of affine transformations of  $\mathbb{C}^d$  such that if  $g \in U$  then  $X \cap gY$  has dimension  $m+n-d$  and is as smooth as possible in that its singular locus is a subset of the union of  $X_{\text{sing}} \cap gY$  with  $X \cap gY_{\text{sing}}$ .

Similarly, Bertini's Theorem states that there is a Zariski open subset  $U$  of the set of polynomials of a fixed degree such that for  $f \in U$ ,  $X \cap \mathcal{V}(f)$  has dimension  $\dim X - 1$  and is as smooth as possible. A consequence of all this is that if  $L$  is a general affine linear subspace of dimension  $d - \dim X$ , then  $X \cap L$  is a finite set of points contained in  $X_{\text{sm}}$ . The number of points is the maximal number of isolated points in any intersection of  $X$  with an affine plane of this dimension and is called the *degree* of  $X$ . These facts underlie the notion of witness set in numerical algebraic geometry from Section 3.

**4.3. Maps.** We often have a map  $\varphi: \mathbb{C}^d \rightarrow \mathbb{C}^n$  given by polynomials, and we want to understand the image of a variety  $X \subset \mathbb{C}^d$  under this map. Algebraic geometry provides a structure theory for the images of polynomial maps. We begin with an example. Consider the hyperbolic paraboloid  $\mathcal{V}(y - xz)$  in  $\mathbb{C}^3$  and its projection to the  $xy$ -plane, which is a polynomial map. This image is the union of all lines through the origin, except for the  $y$ -axis,  $\mathcal{V}(x)$ . Figure 5 shows both the hyperbolic paraboloid and a schematic of its image in the  $xy$ -plane. This image is  $(\mathbb{C}^2 \setminus \mathcal{V}(x)) \cup \{(0, 0)\}$ , the union of a Zariski open subset of  $\mathbb{C}^2$  and the variety  $\{(0, 0)\} = \mathcal{V}(x, y)$ .

A set is *locally closed* if it is open in its closure. In the Zariski topology, locally closed sets are Zariski open subsets of some variety. A set is *constructible* if it is a finite union of locally closed sets. What we saw with the hyperbolic paraboloid is the general case.

**Theorem 4.1.** *The image of a constructible set under a polynomial map is constructible.*

Suppose that  $X \subset \mathbb{C}^d$  and  $\varphi: \mathbb{C}^d \rightarrow \mathbb{C}^n$  is a polynomial map. Then the closure  $\overline{\varphi(X)}$  of the image of  $X$  under  $\varphi$  is a variety. When  $X$  is irreducible, then so is  $\overline{\varphi(X)}$ . (The inverse

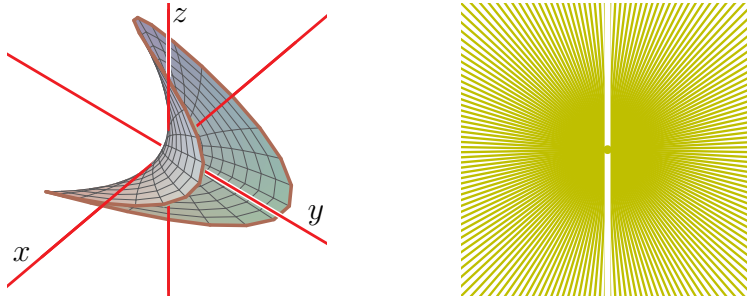


FIGURE 5. The hyperbolic paraboloid and its image in the plane

image of a decomposition  $\overline{\varphi(X)} = Y \cup Z$  under  $\varphi$  is a decomposition of  $X$ .) Theorem 4.1 then implies that  $\varphi(X)$  contains a nonempty Zariski open and therefore a Zariski dense subset of  $\overline{\varphi(X)}$ . Applying this to each irreducible component of a general variety  $X \subset \mathbb{C}^d$  implies that each irreducible component of  $\overline{\varphi(X)}$  has a dense open subset contained in the image  $\varphi(X)$ .

### 5. REAL ALGEBRAIC GEOMETRY

Real algebraic geometry predates its complex cousin, having its roots in Cartesian analytic geometry in  $\mathbb{R}^2$ . Its importance for applications is evident, and applications have driven some of its theoretical development. A comprehensive treatment of the subject is given in the classic treatise of Bochnak, Coste, and Roy [4]. Real algebraic geometry has long enjoyed links to computer science through fundamental questions of complexity. There are also many specialized algorithms for treating real algebraic sets. The equally classic book by Basu, Pollack, and Roy [1] covers this landscape of complexity and algorithms.

**5.1. Algebraic Relaxation.** A complex variety  $X \subset \mathbb{C}^d$  defined by real polynomials has a subset  $X(\mathbb{R}) := X \cap \mathbb{R}^d$  of real points. Both  $X$  and (more commonly)  $X(\mathbb{R})$  are referred to as *real algebraic varieties*. In the Introduction, we claimed that it is fruitful to study a real algebraic variety  $X(\mathbb{R})$  by first understanding the complex variety  $X$ , and then asking about  $X(\mathbb{R})$ . We consider studying the complex variety  $X$  to be an *algebraic relaxation* of the problem of studying the real variety. The fundamental reason this approach is often successful is the following result.

**Theorem 5.1.** *Let  $X \subset \mathbb{C}^d$  be an irreducible variety defined by real polynomials. If  $X$  has a smooth real point, then  $X(\mathbb{R})$  is Zariski dense in  $X$ .*

To paraphrase, suppose that  $X \subset \mathbb{C}^d$  is an irreducible variety defined by real polynomials. If  $X$  has a smooth real point, then all algebraic and geometric information about  $X$  is already contained in  $X(\mathbb{R})$ , and vice-versa.

The reader may have noted that we used pictures of the real algebraic variety  $X(\mathbb{R})$  to illustrate properties of the complex variety  $X$  in most of our figures. Theorem 5.1 justifies this sleight of hand.

A proof of Theorem 5.1 begins by noting that when  $X$  has a smooth real point, then the set of smooth real points  $X_{\text{sm}}(\mathbb{R})$  forms a real manifold of dimension  $\dim X$ . Consequently, the derivatives at a point of  $X_{\text{sm}}(\mathbb{R})$  of a polynomial  $f$  restricted to  $X$  are determined by the restriction of  $f$  to  $X_{\text{sm}}(\mathbb{R})$ , which implies that if a polynomial vanishes on  $X_{\text{sm}}(\mathbb{R})$ , then it vanishes on  $X$ .

The two cones  $\mathcal{V}(x^2+y^2-z^2)$  and  $\mathcal{V}(x^2+y^2+z^2)$  serve to illustrate the hypotheses of Theorem 5.1. In  $\mathbb{C}^3$ , these cones are isomorphic to each other under the substitution  $z \mapsto \sqrt{-1}z$ . In  $\mathbb{R}^3$ , the first is the familiar double cone, with real smooth points the complement of the origin, while the other is the single isolated (and hence singular) point  $\{(0, 0, 0)\}$ . We display the double cone on the left in Figure 6. On the right is the Whitney

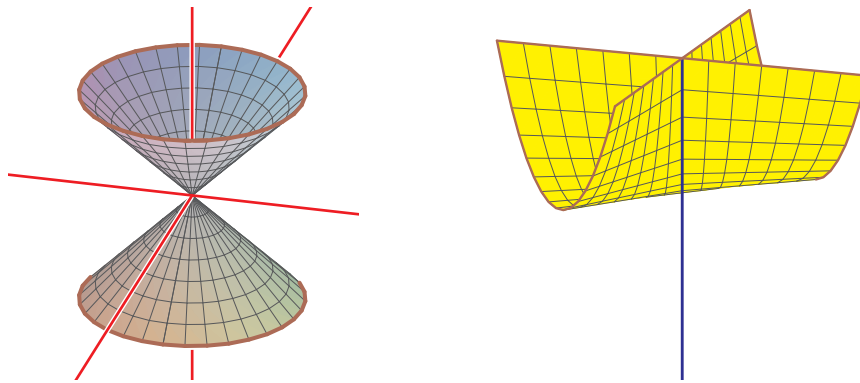


FIGURE 6. Double cone and Whitney umbrella in  $\mathbb{R}^3$

umbrella. This is the Zariski closure of the image of  $\mathbb{R}^2$  under the map  $(u, v) \mapsto (uv, v, u^2)$ , and is defined by the polynomial  $x^2 - y^2z$ . The image of  $\mathbb{R}^2$  is the canopy of the umbrella. Its handle is the image of the imaginary part of the  $u$ -axis of  $\mathbb{C}^2$ , the points  $(\mathbb{R}\sqrt{-1}, 0)$ . The Whitney umbrella is singular along the  $z$ -axis, which is evident as the canopy has self-intersection along the positive  $z$ -axis. This singularity along the negative  $z$ -axis is implied by its having local dimension 1: were it smooth, it would have local dimension 2.

Theorem 5.1 also leads to the following cautionary example. The cubic  $y^2 - x^3 + x$  is irreducible and its set of complex zeroes is a torus (with one point removed). Its set of real zeroes has two path-connected components. Each is Zariski-dense in the complex

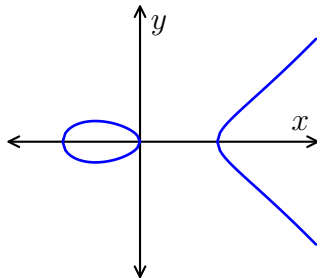


FIGURE 7. Reprise: cubic plane curve



cubic. Thus the property  $x \leq 0$  which holds on the oval is not a generic property, even though it holds on a Zariski dense subset, which is neither Zariski open or closed.

**5.2. Semi-Algebraic Sets.** The image of  $\mathbb{R}^2$  in the Whitney umbrella is only its canopy, and not the handle. More interestingly, the image under projection to the  $xy$ -plane of the sphere  $\mathcal{V}(x^2 + y^2 + z^2 - 1)$  of radius 1 and center  $(0, 0, 0)$  is the unit disc  $\{(x, y) \in \mathbb{R}^2 \mid 1 - x^2 - y^2 \geq 0\}$ . Similarly, by the quadratic formula, the polynomial  $x^2 + bx + c$  in  $x$  has a real root if and only if  $b^2 - 4c \geq 0$ . Thus, if we project the surface  $\mathcal{V}(x^2 + bx + c)$  to the  $bc$ -plane, its image is  $\{(b, c) \in \mathbb{R}^2 \mid b^2 - 4c \geq 0\}$ . We illustrate these examples in Figure 8. They show that the image of an irreducible real variety under a polynomial map need not

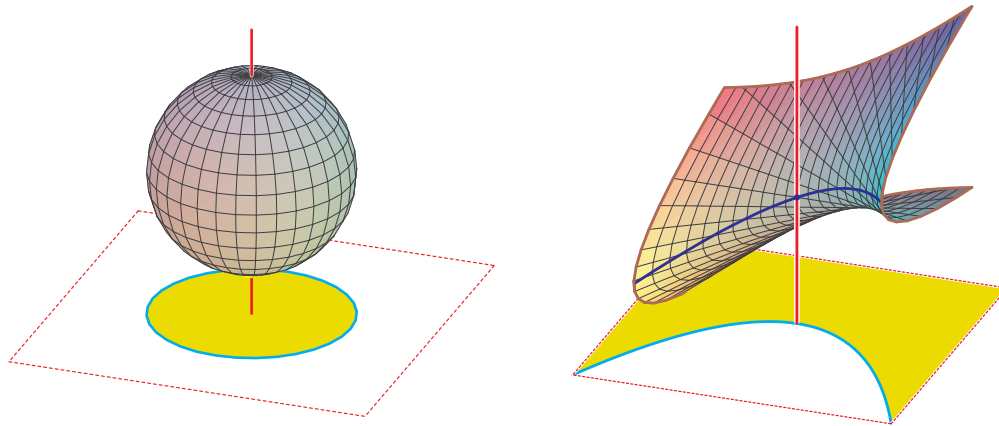


FIGURE 8. Projection of the sphere and the quadratic formula

be dense in the image variety, even though it will be dense in the Zariski topology. We describe the image of a real variety by enlarging our notion of a real algebraic set.

A subset  $V$  of  $\mathbb{R}^d$  is a *semi-algebraic set* if it is the union of sets defined by systems of polynomial equations and polynomial inequalities. Technically, a set  $V$  is semi-algebraic if it is given by a formula in disjunctive normal form, whose elementary formulas are of the form  $f(x) = 0$  or  $f(x) > 0$ , where  $f$  is a polynomial with real coefficients. This is equivalent to  $V$  being given by a formula that involves only the logical operations ‘and’ and ‘or’ and elementary formulas  $f(x) = 0$  and  $f(x) > 0$ . Tarski showed that the image of a real variety under a polynomial map is a semi-algebraic set [20, 21], and Seidenberg gave a more algebraic proof [16].

**Theorem 5.2** (Tarski-Seidenberg). *The image of a semi-algebraic set under a polynomial map is a semi-algebraic set.*

The astute reader will note that our definition of a semi-algebraic set was in terms of propositional logic, and should not be surprised that Tarski was a great logician. The Tarski-Seidenberg Theorem is known in logic as quantifier elimination: its main step is a coordinate projection, which is equivalent to eliminating existential quantifiers.

*Example 5.3.* We give a simple application from rigidity theory. Let  $G$  be a graph with  $n$  vertices  $V$  and  $m$  edges. An embedding of  $G$  into  $\mathbb{R}^d$  is simply a map  $\rho: V \rightarrow \mathbb{R}^d$ , and

thus the space of embeddings is identified with  $\mathbb{R}^{nd}$ . The squared length of each edge of  $G$  in an embedding  $\rho$  defines a map  $f: \mathbb{R}^{nd} \rightarrow \mathbb{R}^m$  with image some set  $M$ . By the Tarski-Seidenberg Theorem,  $M$  is a semi-algebraic set and so it contains an open subset of the real points of its Zariski closure,  $\overline{M}$ . By Sard's Theorem,  $M$  contains a smooth point of its Zariski closure, and thus  $M$  has an open (and dense in the classical topology) set of smooth points. These are images of embeddings where the Jacobian of  $f$  (which is the rigidity matrix) has maximal rank (among all embeddings).  $\diamond$

*Remark 5.4.* Semi-algebraic sets are also needed to describe more general frameworks involving cables and struts. In an embedding, the length of an edge corresponding to a cable is bounded above by the length of that cable. If the edge corresponds to a strut, then the length of that strut is a lower bound for the length of that edge. In either case, inequalities are necessary to describe possible configurations.  $\diamond$

The Tarski-Seidenberg Theorem is a structure theorem for images of real algebraic varieties under polynomial maps. Much later, this existential result was refined by Collins, who gave an effective version of quantifier elimination for semi-algebraic sets, called cylindrical algebraic decomposition [6]. This uses successive coordinate projections to build a description of a semi-algebraic set as a cell complex whose cells are semi-algebraic sets. While implemented in software [5], it suffers more than many algorithms in this subject from the curse of complexity and is most effective in low ( $d \lesssim 3$ ) dimensions. There are however several software implementations of cylindrical algebraic decomposition. In the worst case, the complexity of a cylindrical algebraic decomposition is doubly exponential in  $d$ , and this is achieved for general real varieties. A focus of [1] and subsequent work is on stable algorithms with better performance to compute different representations of a semi-algebraic set.

**5.3. Certificates.** We close with the Positivstellensatz of Stengle [19], which states that a semi-algebraic set is empty if and only if there is a certificate of its emptiness having a particular form. A polynomial  $\sigma$  is a *sum of squares* if it may be written as a sum of squares of polynomials with real coefficients. Such a polynomial takes only nonnegative values on  $\mathbb{R}^d$ . We may use semidefinite programming to determine if a polynomial is a sum of squares.

**Theorem 5.5** (Positivstellensatz). *Suppose that  $f_1, \dots, f_r, g_1, \dots, g_s$ , and  $h$  are real polynomials. Then the semi-algebraic set*

$$(5.1) \quad \{x \in \mathbb{R}^d \mid f_i(x) = 0, i = 1, \dots, r \text{ and } g_j(x) \geq 0, k = 1, \dots, s \text{ and } h(x) \neq 0\}$$

*is empty if and only if there exist polynomials  $k_1, \dots, k_r$ , sums of squares  $\sigma_0, \dots, \sigma_s$ , and a positive integer  $n$  such that*

$$(5.2) \quad 0 = f_1 k_1 + \dots + f_r k_r + \sigma_0 + g_1 \sigma_1 + \dots + g_s \sigma_s + h^{2n}.$$

*Remark 5.6.* To see that (5.2) is a sufficient condition for emptiness, suppose that  $x$  lies in the set (5.1), and then evaluate the expression (5.2) at  $x$ . The terms involving  $f_i$  vanish, those involving  $g_j$  are nonnegative, and  $h(x)^{2n} > 0$ , which is a contradiction. If  $h$  does not appear in a description (5.1), then we take  $h = 1$  in (5.2).  $\diamond$

## 6. GLOSSARY

$\mathbb{C}$ : Complex numbers.

$\mathcal{I}(X)$ : The ideal of a subset  $X$  of  $\mathbb{C}^d$ .

$\mathbb{R}$ : Real numbers.

$\mathcal{V}(S)$ : Set of common zeroes of a collection  $S$  of polynomials.

$X(\mathbb{R})$ : The real points of a variety  $X$  defined by real polynomials.

**constructible**: A set that is a finite union of locally closed sets.

**dimension of  $X$** : The dimension of the smooth (manifold) points of a variety  $X$ .

**general**: A point where a generic property holds.

**generic**: A property that holds on a Zariski open set.

**Gröbner basis**: An algorithmically optimal generating set of an ideal.

**ideal**: Set of polynomials closed under addition and multiplication by other polynomials.

**irreducible variety**: A variety that is not the union of two proper subvarieties.

**real algebraic geometry**: Study of real solutions to systems of polynomial equations.

**real algebraic variety**: A variety defined by real polynomials; its subset of real points.

**semi-algebraic set**: A set defined by a system of polynomial equations and inequalities.

**variety**: A set defined by a system of polynomial equations.

**subvariety**: A variety that is a subset of another.

**Zariski topology**: Topology whose closed sets are varieties.

## REFERENCES

- [1] Saugata Basu, Richard Pollack, and Marie-Françoise Roy, Algorithms in real algebraic geometry, second ed., Algorithms and Computation in Mathematics, vol. 10, Springer-Verlag, Berlin, 2006.
- [2] Daniel J. Bates, Jonathan D. Hauenstein, Andrew J. Sommese, and Charles W. Wampler, Bertini: Software for numerical algebraic geometry, [www.nd.edu/~sommese/bertini](http://www.nd.edu/~sommese/bertini).
- [3] ———, Numerically solving polynomial systems with Bertini, Software, Environments, and Tools, vol. 25, Society for Industrial and Applied Mathematics (SIAM), Philadelphia, PA, 2013.
- [4] Jacek Bochnak, Michel Coste, and Marie-Françoise Roy, Real algebraic geometry, *Ergebnisse der Mathematik und ihrer Grenzgebiete (3)*, vol. 36, Springer-Verlag, Berlin, 1998.
- [5] Christopher W Brown, Qepcad b: a program for computing with semi-algebraic sets using cads, *ACM SIGSAM Bulletin* **37** (2003), no. 4, 97–108.
- [6] George E. Collins, Quantifier elimination for real closed fields by cylindrical algebraic decomposition, Automata theory and formal languages (Second GI Conf., Kaiserslautern, 1975), Springer, Berlin, 1975, pp. 134–183. *Lecture Notes in Comput. Sci.*, Vol. 33.
- [7] David Cox, John Little, and Donal O’Shea, Ideals, varieties, and algorithms, third ed., Undergraduate Texts in Mathematics, Springer, New York, 2007.
- [8] Wolfram Decker, Gert-Martin Greuel, Gerhard Pfister, and Hans Schönemann, SINGULAR 4-0-2 — A computer algebra system for polynomial computations, [www.singular.uni-kl.de](http://www.singular.uni-kl.de), 2015.
- [9] Wolfram Decker and Christoph Lossen, Computing in algebraic geometry, Algorithms and Computation in Mathematics, vol. 16, Springer-Verlag, Berlin, 2006.
- [10] The Sage Developers, Sage Mathematics Software, 2015, [www.sagemath.org](http://www.sagemath.org).
- [11] David Eisenbud, Daniel R. Grayson, Michael Stillman, and Bernd Sturmfels (eds.), Computations in algebraic geometry with Macaulay 2, Algorithms and Computation in Mathematics, vol. 8, Springer-Verlag, Berlin, 2002.
- [12] Daniel R. Grayson and Michael E. Stillman, Macaulay2, a software system for research in algebraic geometry, [www.math.uiuc.edu/Macaulay2/](http://www.math.uiuc.edu/Macaulay2/).

- [13] Jonathan D. Hauenstein and Frank Sottile, Algorithm 921: alphaCertified: certifying solutions to polynomial systems, ACM Trans. Math. Software **38** (2012), no. 4, Art. ID 28, 20.
- [14] Robert Krone and Anton Leykin, NAG4M2: Numerical algebraic geometry for Macaulay 2, [people.math.gatech.edu/~aleykin3/NAG4M2](http://people.math.gatech.edu/~aleykin3/NAG4M2).
- [15] Alexander Morgan, Solving polynomial systems using continuation for engineering and scientific problems, Prentice Hall Inc., Englewood Cliffs, NJ, 1987.
- [16] Abraham Seidenberg, A new decision method for elementary algebra, Ann. of Math. (2) **60** (1954), 365–374.
- [17] Stephen Smale, Newton’s method estimates from data at one point, The merging of disciplines: new directions in pure, applied, and computational mathematics (Laramie, Wyo., 1985), Springer, New York, 1986, pp. 185–196.
- [18] Andrew J. Sommese and Charles W. Wampler, II, The numerical solution of systems of polynomials, World Scientific Publishing Co. Pte. Ltd., Hackensack, NJ, 2005.
- [19] Gilbert Stengle, A nullstellensatz and a positivstellensatz in semialgebraic geometry, Math. Ann. **207** (1974), 87–97.
- [20] Alfred Tarski, A Decision Method for Elementary Algebra and Geometry, RAND Corporation, Santa Monica, Calif., 1948.
- [21] ———, A decision method for elementary algebra and geometry, Quantifier elimination and cylindrical algebraic decomposition (Linz, 1993), Texts Monogr. Symbol. Comput., Springer, Vienna, 1998, pp. 24–84.
- [22] Jan Verschelde, Algorithm 795: PHCpack: general-purpose solver for polynomial systems by homotopy, ACM Trans. Math. Software **25** (1999), no. 2, 251–276.

FRANK SOTTILE, DEPARTMENT OF MATHEMATICS, TEXAS A&M UNIVERSITY, COLLEGE STATION,  
TEXAS 77843, USA

*E-mail address:* [sottile@math.tamu.edu](mailto:sottile@math.tamu.edu)

*URL:* <http://www.math.tamu.edu/~sottile/>